CLAIMS

1. Method for performing an electronic transaction between a first transaction party and a second transaction party using an electronic device operated by the first transaction party, the method comprising:

providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of said electronic device;

providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

activating the authentication software to generate a digital signature from the authentication data;

providing the digital signature to the second transaction party.

2. Method according to claim 1, wherein the second transaction party provides digital data to the first transaction party.

3. Method according to claim 2, wherein the second transaction party embeds the digital signature in the digital data provided to the first transaction party.

4. Method according to claim 1, 2 or 3, wherein the second transaction party stores the digital signature together with data identifying the first transaction party.

5. Method according to any of the preceding claims, wherein the authentication data are provided by the second transaction party, which stores the authentication data together with data identifying the first transaction party.

6. Method according to claim 5, wherein the second transaction party uses the stored authentication data to obtain transaction specific authentication data according to a specific algorithm.

7. Method according to claim 6, wherein the second transaction party verifies the digital signature provided by the first transaction party using the authentication data stored at the second transaction party.

8. Method according to any of the preceding claims, wherein the first transaction party further provides a signed digital signature to the second transaction party, the signed digital signature being

generated by the authentication software by signing the digital signature using a private key, which private key is unique for said authentication software and is known to a third party.

9. Method for performing a verification of legitimate use of digital data on an electronic device, the method comprising:

providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

activating the authentication software to regenerate a digital signature from the authentication data;

providing the digital signature to the authentication software by an application accessing digital data having a digital signature embedded therein; and

comparing the regenerated digital signature with the embedded digital signature.

10. Method according to any of the preceding claims, wherein the authentication data are encrypted by the second transaction party using an encryption key before the authentication data are provided to the first transaction party.

11. Method according to claim 10, wherein the authentication software retrieves a decryption key associated with the encryption key and decrypts the authentication data at its first use.

12. Method according to any of the preceding claims, wherein said memory is inaccessible to an operating system of said electronic device, thereby rendering the authentication data inaccessible to said user.

13. Method according to claim 12, wherein the authentication data are provided in a Basic Input-Output System (BIOS) of the electronic device.

14. Method according to any of the preceding claims, wherein the authentication data are encrypted, when the authentication data are stored in said memory, a decryption key for decrypting the authentication data being inaccessible to said user and to any user-

operated software, thereby rendering the authentication data inaccessible to said user.

15.Method according to claim 14, wherein the authentication data are encrypted using at least two encryption layers.

16.Method according to claim 15, wherein at least one encryption layer may be decrypted using a decryption key associated with one or more serial numbers of hardware components of said electronic device.

17.Method according to claim 15 or 16, wherein at least one encryption layer may be decrypted by the authentication software.

18.Method according to any of claims 14 - 17, wherein the authentication data are decrypted in a secure processing environment inaccessible to said user and to any user-operated software.

19.Method according to any of the preceding claims, wherein the authentication data comprise an authentication table.

20.Method according to claim 19, wherein the authentication table is generated from a bit string which is generated from fixed data and variable data.

21.Method according to claim 20, wherein the fixed data are at least part of a serial number of a hardware device.

22.Method according to claim 20, wherein the fixed data are at least part of a device specific software identification code of the authentication software.

23.Method according to claim 20, 21 or 22, wherein the variable data comprise a random table.

24.Method according to claim 23, wherein the random table is calculated from a random two-dimensional or three-dimensional pattern.

25.Method according to any of claims 19 - 24, wherein the authentication table is generated from fixed data, variable data and a bit string, which bit string is specific to a trusted third party that provides the authentication data.

26.Method according to any of the preceding claims, wherein the authentication software is stored in a secure memory location inaccessible to an operating system.

27.Method according to any of the preceding claims, wherein the authentication software is run in a secure processing environment inaccessible to an operating system.

28.Method for encrypting digital data on an electronic device using an encryption key, the method comprising:

gathering session specific data;

hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device;

generating said encryption key from the characters stored in the authentication table at said positions; and

encrypting said digital data using said encryption key.

29.System for performing an electronic transaction between a first transaction party and a second transaction using an electronic device operated by the first transaction party, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate a digital signature from the authentication data;

means for providing the digital signature to the second transaction party; and

means for providing digital data from the second transaction party to the first transaction party.

30.System for performing a verification of legitimate use of digital data on an electronic device, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate a digital signature from the authentication data;

means for providing the digital signature to the authentication software by an application accessing digital data having a digital signature embedded therein; and

means for comparing the regenerated digital signature with the embedded digital signature.

31.System for encrypting digital data using an encryption key, the system comprising:

means for providing authentication data in a memory of said electronic device which authentication data are inaccessible to a user of the electronic device;

means for providing authentication software in said electronic device, the authentication data being accessible to said authentication software;

means for activating the authentication software to generate a digital signature from the authentication data;

means for gathering session specific data;

means for hashing said session specific data to obtain reference numbers referring to positions in an authentication table stored in said electronic device;

means for generating said encryption key from the characters stored in the authorization table at said positions; and

means for encrypting said digital data using said encryption key.